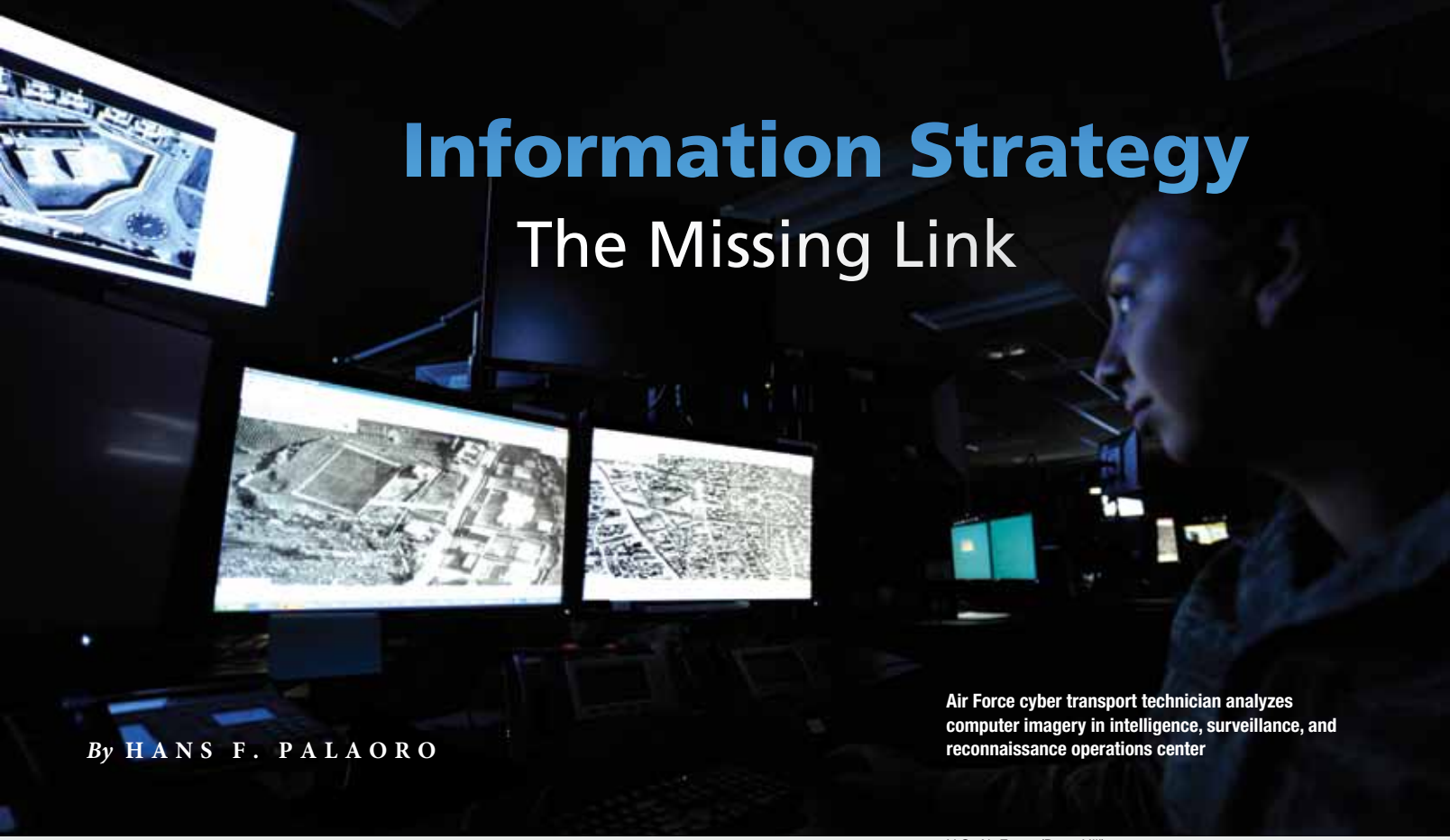
Information Strategy
The Missing Link



Air Force cyber transport technician analyzes computer imagery in intelligence, surveillance, and reconnaissance operations center

U.S. Air Force (Dana Hill)

By HANS F. PALAORO

Success will be less a matter of imposing one's will and more a function of shaping behavior.

—Secretary of Defense Robert M. Gates[1]

IO is dead! Long live IO! After 13-plus years of infighting, programmatic protectionism, general angst over who owns what, and turf battles with its new sibling the cyber community, a new draft doctrinal definition of information operations (IO) is now working its way through the Pentagon. Unlike previous definitions that centered on what things IO *owns* (the "pillars" and later the "core capabilities" of electronic warfare, computer network operations, psychological operations, military deception, and operations security), the new definition omits such lists, focusing instead on what IO *does*.[2]

Lieutenant Colonel Hans F. Palaoro, USAF, wrote this essay while a student at the Industrial College of the Armed Forces. It won the Strategy Article category of the 2010 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

Information operations are "the planning and integrated employment of capabilities in the information environment across the phases of joint military operations."[3] This new definition avoids the major pitfall of its predecessors—a rice-bowl approach that actually *discouraged* integration of efforts. But this article is not about whether that new definition is right, or even good. It is about how the door is now open for a fresh look at an even more significant issue.

The world of IO has always had a weakness: the endless doctrinal debate about "who owns what" has distracted from useful discussion on how to orchestrate those pieces to actually accomplish something—in other words, *strategy*. Just what are the *ends*, *ways*, and *means* of IO, and how do we align them to defeat an enemy? The Department of Defense (DOD)—in fact, the U.S. Government as a whole—desperately needs a construct for designing interagency *offensive information strategy* that will enable leaders to employ the information element of national power in military operations. To build one, we first look at where current thought on "information power" is lacking. Then we walk through the elements of an IO strategy. The desired ends are unexpectedly simple: either *adversary behavior has changed*, or *further resistance is impossible*. Then we use a new construct for binning the means: *hard* and *soft* tools. Finally, we bridge the gap between those two with the ways—using the soft tools to *influence*, and the hard tools to *disrupt*, enemy action. We start with some basics.

Information Power

While information power is well accepted as one of the four elements of national power, neither the term nor the concept appeared in the 2006 National Security Strategy. It is strangely absent from the "full array of political, economic, diplomatic, and other tools at our disposal" that is the basis of the document.[4] Nor does information power appear in the 2008 National Defense Strategy.[5] Moreover, although there is no vetted definition of information power, the concept is understood and the link to how the military should exercise it is obvious: information operations. Considerable attention has

the desired ends are simple: either adversary behavior has changed, or further resistance is impossible

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Strategy: The Missing Link	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University Press,Joint Force Quarterly,260 Fifth Ave., Bldg. 64, Fort McNair,Washington,DC,20319-5066**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**3**	


DOD (Cherie Cullen)

Commander, U.S. Strategic Command, speaks at activation of U.S. Cyber Command

already been given to the "defensive" side of the information domain.[6] What is still lacking is the offense.

The problem with the current IO model is that it fails to orchestrate the tools of information power toward a common goal. One reason is that the legal and bureaucratic limits on who can do certain things have caused an almost irrational phobia *against* integrated efforts. For example, fear of cross-contamination of public affairs (PA), public diplomacy (PD), and strategic communication with psychological operations (PSYOP) actively opposes effective coordination of these obviously interdependent tools of information strategy.

Similarly, while military doctrine does recognize the existence of tools such as PD, it essentially stiff-arms them: "Their primary purpose and rules under which they operate must not be compromised by IO."[7] In this way, current doctrine only guarantees that whatever plan comes out will lack interagency collaboration—the recipe for strategic failure. Information power *is* multiagency. The State Department does slightly better. State's U.S. National Strategy for Public Diplomacy and Strategic Communication at least recognizes that "key influencers" include "military personnel" and that PD efforts must make use of them.[8] While that is a nice nod to recognizing the issue, it is not a solution. In neither DOD doctrine nor State Department "strategy" do we find a concept for linking IO ends, ways, and means.

To accomplish that, we should first define the target. The target of offensive IO is the mind of the adversary. During conflict, especially during phases two (deter) and three (seize initiative) of a campaign, the primary target is the mind of the enemy commander at every level, from the national dictator down to the infantry company commander. Other targets may include the minds of lesser officials, the local populace, and outside actors. During other phases, the relative importance of each of those targets will vary. For instance, during phase four (dominate), the minds of the populace may be more important than the minds of any remaining militant commanders. Given that target—the adversary mind—we can now devise strategy.

Offensive Information Strategy

Contrary to standard assumptions about how complicated IO is, there are just two basic ends for any offensive information strategy: *the adversary's behavior has changed*, or *further coordinated resistance by that adversary is impossible*. All interagency plans and actions in the information domain must be aligned to accomplish one of those ends. In the first case, the desired end is for adversary decisionmakers, commanders, and populations to voluntarily capitulate to or implement our demands. Defining precisely what specific adversary behavior must change (often "cessation of aggression" or "surrender") will vary from conflict to conflict, but in all cases it is the crucial first step.

When approached in this way, it becomes clear that this end of information operations is actually the *supported*, not a supporting, operation, around which the other diplomatic, informational, military, and economic elements must be aligned.[9] In the second case, the desired end is that the adversary's ability to command and control forces and effectively resist will have collapsed. Seeking this end normally implies that the first end has not been achieved, making it a supporting, rather than supported, operation. The situation and phase of operations will dictate which of those two ends has primacy. But before we look at how, let us first look at the available means.

Means, Ways, and Ends

The *means* of IO are comprised of two sets of tools: the hard tools that (probably) constitute acts of war, and the soft tools that (probably) do not. The hard tools include computer network attack (CNA), electronic attack (EA), and kinetic attack. The soft tools include not only the traditional military capabilities of PSYOP and military deception, but also strategic communication, PA, and PD. While some may feel uncomfortable about putting these all together into one strategy, *not* doing so is precisely what has been getting in the way. Until we put all the tools on the table and force interagency collaboration, IO will remain forever fragmented.

This brings us to the *ways*: how to link the means to the ends. The existing doctrinal diagrams, with their "pillars" and "capabilities," do nothing to show how to align them toward desired ends. That requires a new framework integrating the means across interagency boundaries. If the ends of IO strategy are "changed behavior" and "inability to resist," then the *ways* also become clear. The means—the tools of IO—must be used either to *influence* or to *disrupt* the adversary.[10] For influence, the soft tools are most applicable here, and the IO strategist must orchestrate the interagency owners and actors to align them (see figure 1). PD and PSYOP must complement each other in their efforts to change adversary behavior, and military deception must reinforce them both. Most importantly, we must align our IO

until we put all the tools on the table and force interagency collaboration, IO will remain forever fragmented

efforts with our actions—the "diplomacy of the deed."

As far as disruption, we find a model readily available in John Boyd's oft-trivialized "OODA Loop" (observe, orient, decide, act). In fact, Boyd's entire concept—of late, usually misunderstood to mean that we simply need to speed up our own decision processes to guarantee victory—argued that by disrupting the enemy's ability to make decisions, we would cause complete collapse of effective command.[11] By applying the hard tools of CNA, EA, and kinetic attack, supplemented by the soft tools, to disrupt the adversary's OODA loops and command and control systems at appropriate points (see figure 2), we can quickly render organized resistance impossible.

Overcoming more than a decade of IO inability to deliver will take some new thought and direction. The proposed new definition of IO is a helpful start, but it does not fill the need for an offensive information strategy model. For that we must reorganize strategy along the lines of ends, ways, and means. The ends are simple: adversary behavior has changed, or further adversary resistance is impossible. The means bin nicely into two groups, the hard and soft tools. Finally, the ways tie them all together using the soft tools to *influence* and the hard tools to *disrupt* the adversary. Using this model, we will finally be able to effectively apply the information element of power in offensive operations. **JFQ**

Figure 1. Orchestrating the Ends, Ways, and Means of Information Operations Strategy

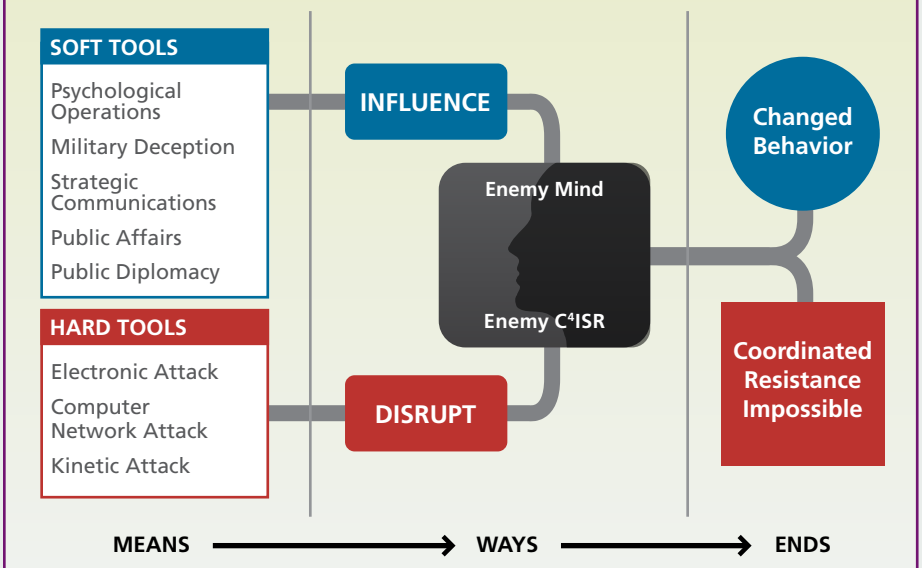
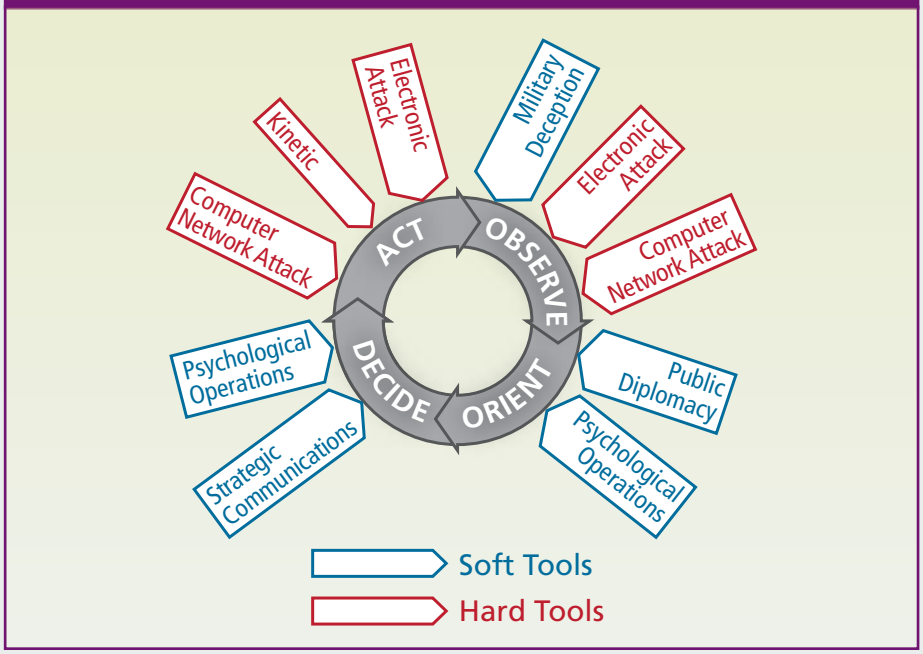


Figure 2. Using Information Operations Tools to Disrupt OODA Loop



NOTES

[1] Quoted in Paul J. Granetto, *Information Operations Career Force Management* (Arlington, VA: Department of Defense Inspector General, 2009), 1, available at <www.dodig.mil/Audit/reports/fy09/09-090.pdf>.

[2] Walter L. Sharp, Joint Publication 3–13, *Information Operations* (Norfolk, VA: Joint Warfighting Center, Doctrine and Education Group, 2006), iii, available at <www.dtic.mil/doctrine/new_pubs/jp3_13.pdf>.

[3] "Information Operations" (Washington, DC: Staff action package, Office of the Under Secretary of Defense [Intelligence], 2009), 1. The six phases of joint military operations are one—shape; two—deter; three—seize the initiative; four—dominate; five—stabilize; six—enable civil authority.

[4] George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2006), 6, available at <www.strategicstudiesinstitute.army.mil/pdffiles/nss.pdf>.

[5] Robert M. Gates, *National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2008), 2, available at <www.defenselink.mil/pubs/2008NationalDefenseStrategy.pdf>.

[6] Richard A. Clarke, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0* (Washington, DC: Critical Infrastructure Assurance Office, 2000), vi, available at <www.fas.org/irp/offdocs/pdd/CIP-plan.pdf>.

[7] Sharp, x.

[8] Karen Hughes and Policy Coordinating Committee, *U.S. National Strategy for Public Diplomacy and Strategic Communication* (Washington, DC: Department of State, 2007), 4, available at <www.state.gov/documents/organization/87427.pdf>.

[9] William M. Darley, "Clausewitz's Theory of War and Information Operations," *Joint Force Quarterly* 40 (1st Quarter, 2006), 73–79.

[10] When applied to an actual operation, clear goals and objectives of influence must be specified early on: *who* must be influenced to *do* or *think* what?

[11] John R. Boyd, *A Discourse on Winning and Losing* (Maxwell Air Force Base, AL: Air University, 1987).